



powered by AirVPN

This is the kind of information that all the sites you visit, as well as their advertisers and any embedded widget, can see and collect about you.

Your IP addresses

23.226.129.58

United States - New Jersey

No forwarded IP detected. If you are using a proxy, it's a transparent proxy.

● IPv6 test not reachable. (error)

Browser default: ● IPv4 (2376 ms)

Fallback: ● Fail (error)

Your IP addresses - WebRTC detection

DNS Addresses - 53 servers, 1 tests pending

74.125.18.66



United States - District of Columbia

74.125.18.67



United States - District of Columbia

172.253.10.5



United States - District of Columbia

172.253.210.75



United States - District of Columbia

172.253.8.4



United States - District of Columbia

74.125.18.65



United States - District of Columbia

172.253.214.6



United States - District of Columbia

172.253.210.69



United States - District of Columbia

74.125.18.68



United States - District of Columbia

172.253.214.14



United States - District of Columbia

172.253.210.78



United States - District of Columbia

172.253.9.3



United States - District of Columbia

173.194.168.194



United States - District of Columbia

172.253.8.5



United States - District of Columbia

172.253.210.73



United States - District of Columbia

172.253.214.9



United States - District of Columbia

74.125.18.1



United States - District of Columbia

172.253.210.70



United States - District of Columbia

172.253.10.3



United States - District of Columbia

172.253.9.4



United States - District of Columbia

172.253.8.3



United States - District of Columbia

172.253.214.99



United States - District of Columbia

74.125.18.69



United States - District of Columbia

172.253.214.110



United States - District of Columbia

172.253.10.4



United States - District of Columbia

172.253.10.1



United States - District of Columbia

172.253.214.1



United States - District of Columbia

172.253.214.102



United States - District of Columbia

74.125.18.2



United States - District of Columbia

172.253.8.2



United States - District of Columbia

172.253.210.71



United States - District of Columbia

172.253.9.2



United States - District of Columbia

172.253.214.105



United States - District of Columbia

172.253.210.65



United States - District of Columbia

173.194.168.195



United States - District of Columbia

74.125.18.4



United States - District of Columbia

172.253.10.2



United States - District of Columbia

172.253.214.111



United States - District of Columbia

172.253.214.108



United States - District of Columbia

172.253.214.101



United States - District of Columbia

172.253.214.12



United States - District of Columbia

172.253.214.7



United States - District of Columbia

173.194.168.196



United States - District of Columbia

172.253.214.11



United States - District of Columbia

172.253.214.109



United States - District of Columbia

172.253.214.107



United States - District of Columbia

172.253.214.104



United States - District of Columbia

172.253.214.97



United States - District of Columbia

172.253.214.103



United States - District of Columbia

172.253.210.74



United States - District of Columbia

172.253.214.106



United States - District of Columbia

172.253.210.79



United States - District of Columbia

United States - District of Columbia

If you are now connected to a VPN and between the detected DNS you see your ISP DNS, then your system is [leaking DNS requests](#)

Torrent Address detection

[Activate](#)

Geolocation detection

[Activate](#) (may prompt an user permission on the browser)

IP Details

IP: 64.18.9.207

[AirVPN](#) Exit Node:  No

Country:  United States (US)

Region: New York (NY)

City: New York

Metro (US-Only): 501

Time Zone: America/New_York

Latitude & Longitude: 40.8171 , -73.9392

Detected informations

Your User Agent: Mozilla/5.0 (X11; CrOS x86_64
13310.93.0) AppleWebKit/537.36
(KHTML, like Gecko)
Chrome/85.0.4183.133 Safari/537.36

What document you can accept: text/html, application/xhtml+xml,
application/xml;q=0.9, image/avif,
image/webp, image/apng, */*;q=0.8,
application/signed-exchange;v=b3;q=0.9

What

System information

(your browser, your language, your operating system, etc)

Platform: Linux x86_64

Cookie enabled: true

Java enabled: false

Online: true



[View Larger Map](#)

Accuracy Radius: 20 KM

Last data update: Sat, 10 Oct 2020 00:04:56 +0000

Geek Details

Screen information

(your display hardware)

Your screen: 1920 x 1080

Available screen: 1920 x 1032

Color depth: 24

Pixel depth: 24

Plugins information

(your browser plugins)

Name: Chrome PDF Plugin

File name: internal-pdf-viewer

Description: Portable Document Format

Name: Chrome PDF Viewer

File name: mhjfbmdgcfjbbpaeojofohoeftgiehjai

Name: Native Client

Mime-Types information

(what document you can read)

Mime Type: application/msexcel

Extensions: *

Plugin: Office Editing for Docs, Sheets & Slides

Mime Type: application/mspowerpoint

Extensions: *

Plugin: Office Editing for Docs, Sheets & Slides

HTTP Request Headers

Accept-Language: en-US, en;q=0.9

Accept-Encoding: gzip, deflate, br

Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

What are WebRTC leaks?

WebRTC implement STUN (Session Traversal Utilities for Nat), a protocol that allows to discover the public IP address. To disable it:

- Mozilla Firefox: Type "about:config" in the address bar. Scroll down to "media.peerconnection.enabled", double click to set it to false.
- Google Chrome: Install Google official extension [WebRTC Network Limiter](#).
- Opera: Type "about:config" in the address bar or go to "Settings". Select "Show advanced settings" and click on "Privacy & security". At "WebRTC" mark select "Disable non-proxied UDP".

What are DNS leaks?

In this context, with "DNS leak" we mean an unencrypted DNS query sent by your system OUTSIDE the established VPN tunnel.

Why does my system leak DNS queries?

In brief: Windows lacks the concept of global DNS. Each network interface can have its own DNS. Under various circumstances, the system process svchost.exe will send out DNS queries without respecting the routing table and the default gateway of the VPN tunnel, causing the leak.

Should I be worried for a DNS leak?

If you don't want that your ISP, and anybody with the ability to monitor your line, knows the names your system tries to resolve (so the web sites you visit etc.) you must prevent your system to leak DNS. If you feel that you're living in a human rights hostile country, or in any way the above mentioned knowledge may harm you, you should act immediately to stop DNS leaks.

How does torrent detection work?

To detect data from your torrent client we provide a magnet link to a fake file. The magnet contains an http url of a controlled by us tracker which archives the information coming from the torrent client.

Service available on [IPv4](#) and [IPv6](#). Look at [the forum](#) for support, feedback, API.

Data partially based on [MaxMind](#) database. Results may be cached, refer to MaxMind for more accuracy.

powered by  **AirVPN**